



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/001,410	10/31/2001	George S. Gales	10017028-1	3057

7590 12/22/2005  
HEWLETT-PACKARD COMPANY  
Intellectual Property Administration  
P.O. Box 272400  
Fort Collins, CO 80527-2400

EXAMINER

SHERKAT, AREZOO

ART UNIT PAPER NUMBER

2131

DATE MAILED: 12/22/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	Application No. 10/001,410	Applicant(s) GALES ET AL.	
	Examiner Arezoo Sherkat	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 26 September 2005.
- 2a) ☒ This action is **FINAL**.      2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-27 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-27 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

***Response to Amendment***

This office action is responsive to Applicant's amendment received on Sep. 26, 2005. Claims 1-5, 12, and 20-27 are amended. Claims 1-27 are pending.

***Response to Arguments***

Applicant's arguments with respect to claims 1-27 have been considered but are moot in view of the new ground(s) of rejection.

***Claim Rejections - 35 USC § 103***

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-27 are rejected under 35 U.S.C. 103(a) as being unpatentable over Chefalas et al., (U.S. Publication No. 2002/0116639 and Chefalas hereinafter), in view of Hill et al., (U.S. Patent No. 6,088,804 and Hill hereinafter).

Regarding claims 12, 1, and 2, Chefalas discloses a method of defining the security vulnerability of a computer system, comprising:

generating a human-readable and a machine-readable vulnerability description language (VDL) file (i.e., Network Status Display 42) specifying: an attack representing a recognized vulnerability of the computer system, at least one attribute of the specified

attack (i.e., virus name), and a remedy for the specified vulnerability (i.e., action to be taken to mitigate the attack) (Page 4, Par. 0047-0048).

Chefalas does not expressly disclose specifying specifying at least one policy definition with respect to detecting the vulnerability of the specified attack.

However, Hill discloses specifying at least one policy definition with respect to detecting the vulnerability of the specified attack (i.e., attack signature log 110)(Col. 8, lines 62-67 and Col. 9, lines 1-25).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Chefalas with teachings of Hill because it would allow to include specifying at least one policy definition with respect to detecting the vulnerability of the specified attack as disclosed by Hill. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Hill to provide for the ability to evolve with evolving threats to effectively mitigate new approaches to network attacks (Hill, Col. 2, lines 55-60).

Regarding claims 3 and 13, Chefalas discloses further comprising generating the VDL file specifying a computing platform of the computer system (Page 4, Par. 0047).

Regarding claims 4 and 14, Chefalas discloses further comprising:  
specifying a security category of the specified attack, and specifying at least one policy group with respect to the specified security category (Page 4, Par. 0046).

Regarding claims 5 and 15, Chefalas discloses further comprising generating the VDL file specifying a vulnerability scanner executing on the computer system (Page 2, Par. 0027-0028).

Regarding claims 6 and 16, Chefalas does not expressly disclose specifying an identification of the severity associated with a breach of the computer system by the attack.

However, Hill discloses wherein specifying at least one attribute of the specified attack comprises specifying an identification of the severity associated with a breach of the computer system by the attack (Col. 5, lines 20-67 and Col. 6, lines 1-23).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Chefalas with teachings of Hill because it would allow to include specifying at least one policy definition with respect to detecting the vulnerability of the specified attack as disclosed by Hill. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Hill to provide for the ability to evolve with evolving threats to effectively mitigate new approaches to network attacks (Hill, Col. 2, lines 55-60).

Regarding claim 7, Chefalas discloses wherein specifying at least one attribute of the specified attack comprises specifying a description of the attack (Page 5, Par. 0060).

Regarding claims 8 and 17, Chefalas discloses wherein specifying at least one attribute of the specified attack comprises specifying an explanation of why the specified attack is important (i.e., to prevent the occurrence of this type of event in future)(Page 5, Par. 0059).

Regarding claims 9 and 18, Chefalas discloses wherein specifying at least one attribute of the specified attack comprises specifying how information is to be reported to a user with respect to the specified attack (i.e., notification to the manager, the administrator, or a technician)(Page 4, Par. 0047 and Page 5, Par. 0060).

Regarding claims 10, 19, and 27, Chefalas discloses wherein specifying at least one attribute of the specified attack comprises specifying a source of a remedy operable to fix the specified vulnerability (Page 5, Par. 0054-0058).

Regarding claim 11, Chefalas discloses wherein specifying at least one attribute of the specified attack comprises specifying information to enable a manual remedy of the specified vulnerability (Page 5, Par. 0060-0062).

Regarding claim 20, Chefalas discloses a system of defining security vulnerabilities of a computer system, comprising:

generating a human-readable and a machine-readable vulnerability description language (VDL) file specifying: an attack representing a recognized vulnerability of the computer system, at least one attribute of the specified attack (i.e., virus name), and a remedy for the specified vulnerability (i.e., action to be taken to mitigate the attack) (Page 4, Par. 0047-0048).

an interpreter operable to parse the at least one vulnerability definition and at least one policy item definition in the VDL file and organize the parsed definitions pursuant to a predetermined format (Page 2-3, Par. 0025-0032), and a data storage operable to store the parsed and organized at least one vulnerability and at least one policy item definition, wherein the data storage is accessible by at least one vulnerability scanner application (Page 4, Par. 0044-0048).

Chefalas does not expressly disclose a definition of at least one policy item for detecting the vulnerability in the VDL file (i.e., policy 500 and 502).

However, Hill discloses wherein a human-readable and machine-readable vulnerability description language (VDL) file (i.e., Network Status Display 42) containing a definition of at least one vulnerability (i.e., security event type and location 108) and a definition of at least one policy item for detecting the vulnerability (i.e., attack signature log 110)(Col. 8, lines 62-67 and Col. 9, lines 1-25).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Chefalas with teachings of Hill

because it would allow to include specifying at least one policy definition with respect to detecting the vulnerability of the specified attack as disclosed by Hill. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Hill to provide for the ability to evolve with evolving threats to effectively mitigate new approaches to network attacks (Hill, Col. 2, lines 55-60).

Regarding claim 21, Chefalas discloses wherein the data storage is a relational database having a plurality of tables (Page 4, Par. 0046-0048).

Regarding claim 22, Chefalas discloses wherein the VDL file further comprises a definition of a vulnerability scanner application (i.e., instruction)(Page 4, Par. 0045).

Regarding claim 23, Chefalas discloses wherein the VDL file further comprises a definition of a security category providing a grouping of the at least one vulnerability, and a definition of a policy group providing a grouping of the at least one policy item (Page 4, Par. 0046).

Regarding claim 24, Chefalas discloses wherein the VDL file further comprises a definition of at least one attribute of the at least one vulnerability (i.e., virus name)(Page 4, Par. 0043-0044).



Regarding claim 25, Chefalas does not expressly disclose wherein the VDL file further comprises an identification of the severity of risk associated with the at least one vulnerability.

However, Hill discloses wherein specifying at least one attribute of the specified attack comprises specifying an identification of the severity associated with a breach of the computer system by the attack (Col. 5, lines 20-67 and Col. 6, lines 1-23).

Therefore, it would have been obvious to a person of ordinary skill in the art at the time of applicant's invention to modify teachings of Chefalas with teachings of Hill because it would allow to include specifying at least one policy definition with respect to detecting the vulnerability of the specified attack as disclosed by Hill. This modification would have been obvious because one of ordinary skill in the art would have been motivated by the suggestion of Hill to provide for the ability to evolve with evolving threats to effectively mitigate new approaches to network attacks (Hill, Col. 2, lines 55-60).

Regarding claim 26, Chefalas discloses wherein the VDL file further comprises a definition of how information is to be displayed to a user with respect to the at least one vulnerability (i.e., notification to the manager, the administrator, or a technician)(Page 4, Par. 0047 and Page 5, Par. 0060).

***Conclusion***

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Arezoo Sherkat whose telephone number is (571) 272-3796. The examiner can normally be reached on 8:00-4:30 Monday-Friday.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2131

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



Arezoo Sherkat  
Patent Examiner  
Group 2131  
Dec. 15, 2005

  
Primary Examiner  
AV231  
12/15/05